Chapter 12: Kerberos Command Descriptions

In this chapter we list the native Kerberos commands, and provide a brief description and option list with descriptions adapted from the man pages. Programs that Kerberos provides for ticket and password management include **kinit**, **klist**, **kpasswd** and **kdestroy**.

12.1 kinit

`kinit` obtains and caches a ticket (a ticket-granting ticket, by default) for the default principal or for a specified principal.

12.1.1 Syntax

```
% kinit [-A] [-c cache_name] [-f] [-F] [-g [-h] | G]\
 [-k [-t keytab_file]] [-l lifetime] [-p] [-P]\
 [-r renewable_life] [-R] [-s start_time] [-S service_name]\
 [-v] [-V] [-4] [-5] [principal]
```

12.1.2 Option Descriptions

`-A` requests addressless ticket (used to obtain a Kerberos ticket not bound to a particular IP address, which can then be passed through a NAT-created "firewall"; see section 6.5 *Network Address Translation*).

`-c <cache_name>`

uses **`<cache_name>`** as the credentials (ticket) cache name and location; if this option is not used, the default cache name and location are used.

The default credentials cache may vary by system. If the KRB5CCNAME environment variable is set, its value is used to name the default ticket cache. At Fermilab, this

variable is typically set to **FILE:/tmp/krb5cc_<some_string>**. Any existing contents of the cache are destroyed by **kinit**.

-f requests forwardable tickets

-F requests nonforwardable tickets

-g runs **aklog** after obtaining tickets; if you choose this, you may also choose **-h**.

-G does not run **aklog** after obtaining tickets

-h does AFS aklog setpag (goes with **-g**)

-k [-t <keytab_file>]

requests a host ticket, obtained from a key in the local host's keytab file. The name and location of the keytab file should be specified with the **-t <keytab_file>** option; otherwise the default name and location will be used (the default `/etc/krb5.keytab` is not useful here (except to *root*); users cannot read it). Keytab files are generally used for service principals. They are also used for **cron** jobs (see section 10.3.1 *Specific-User Processes (cron Jobs)*).

-l <lifetime> requests a ticket with the lifetime **<lifetime>**. The value for **<lifetime>** must be a number followed immediately by a delimiter indicating the unit of time, as follows:

<n>s (seconds)

<n>m (minutes)

<n>h (hours)

<n>d (days)

For example: **kinit -l 90m**. You cannot mix units; e.g., a value of "**-l 1h30m**" will result in an error.

If the **-l** option is not specified, the default ticket lifetime (26 hours, at Fermilab) is used. This option is only useful for specifying a ticket lifetime shorter than the default; to extend the lifetime beyond this limit you must renew the ticket; see **-r** and **-R**.

-p requests proxiable tickets

-P requests nonproxiable tickets

-r <renewable_life>

requests renewable tickets, with a maximum lifetime of **<renewable_life>**. If given a value longer than the preconfigured seven day limit, it will be set to seven days. **<renewable_life>** uses the same format as the **<lifetime>** associated with the **-l** option, with the same delimiters.

-R requests renewal of the renewable ticket. Renewal must take place before the ticket's lifetime expires. An expired ticket cannot be renewed, even if the ticket is still within its renewable life.

-s <start_time>

requests a postdated ticket, which can be validated (by action of the user) any time after **<start_time>**. Its lifetime starts when it gets validated. Format for the date and time can be any of the following:

yyyymmddhhmmss

yyyy.mm.dd.hh.mm.ss

yymmddhhmmss

yy.mm.dd.hh.mm.ss

yymmddhhmm

hhmmss

hhmm

hh:mm:ss

hh:mm

Postdated tickets are issued with the "invalid" flag set, and need to be validated before use; see **-v**.

-S <service_name>

specifies a particular service name to use when getting initial tickets. If this option is not used, you get a ticket-granting-ticket by default.

-v requests that the post-dated ticket in the cache (with the "invalid" flag set) be passed to the KDC for validation. If the start time has passed, the cache is replaced with the validated ticket.

-V displays verbose output

-4 gets Kerberos v4 tickets only; by default get v5 only

-5 gets Kerberos v5 tickets only (default)

12.1.3 Examples

Default

Typically you can run the **kinit** command without options. This gets you a 26-hour ticket with the flags FIA set by default (Forwardable, Initial, Preauthenticated; flags are viewable using **klist -f**, see section 12.2 *klist*), plus an AFS token if AFS is running on the machine.

Get Ticket with Specified Lifetime

Request a ticket valid for three hours using the **-l** option:

```
% kinit -l 3h
```

Get Renewable Ticket

Using the **-r** option, request a renewable ticket with a maximum renewable lifetime of four days (this sets the R flag on the ticket for Renewable, and sets the AFS token lifetime to four days):

```
% kinit -r 4d
```

Then, before the lifetime of 26 hours has passed, and before four days expire (you can renew a ticket multiple times within its renewable lifetime, but not after it has expired), renew the ticket using the **-R** option:

```
% kinit -R
```

The ticket will remain active an additional 26 hours or until its original four days expires, whichever comes first.

Get Postdated Ticket

Next, request a postdated ticket (using the **-s** option), with a lifetime of six hours (the lifetime starts at validation time):

```
% kinit -s 12:25 -l 6h
```

Until it gets validated, the invalid ticket has the flags FdiIA set by default, where d is PostDated and i is Invalid. Validate it after the start time has passed (using the **-v** option):

```
% kinit -v
```

Get Ticket based on Key

The following command requests a TGT for the principal project/group/host.fnal.gov, for the duration 30 minutes, with authentication done on the basis of a key previously stored in the keytab file

`/usr/tmp/project.keytab` (this command would normally be included in a **cron** job file, not run interactively; see section 10.3.1 *Specific-User Processes (cron Jobs)*):

```
% kinit -l 30m -k -t /usr/tmp/project.keytab \
  project/group/host.fnal.gov
```

If you have an automatic process running as *root*, it is simplest to consider that the host on which the job runs is the party responsible for the accesses it initiates, and have it use the `/etc/krb5.keytab` to obtain credentials as `host/<hostname>.<domain>`:

```
% kinit -l 30m -k host/<hostname>.<domain>
```

12.2 klist

`klist` lists the Kerberos principal and Kerberos tickets held in a credentials cache (the default), or lists the keys held in a keytab file.

12.2.1 Syntax

```
% klist [-e] [[-c] [[-f] [-s] [-a [-r]] [<cache_name>] ]]\
  [-k [-t] [-K] [<keytab_name>]] [-4] [-5]
```

12.2.2 Option/Argument Descriptions

`-a`	displays the address list. Requires **`-c`**. Invalid with **`-k`**.
`-c`	lists tickets held in a credentials cache (as opposed to keys in a keytab file). Invalid with **`-k`**. This is the default if neither **`-c`** nor **`-k`** is specified.
`<cache_name>`	specifies the credentials cache. If **`<cache_name>`** is not specified, **`klist`** will display the credentials in the default credentials cache (unless instructed to operate on a keytab file). If the KRB5CCNAME environment variable is set, its value is used to name the default ticket cache. At Fermilab, this variable is typically set to **`FILE:/tmp/krb5cc_<some_string>`**. Requires **`-c`**. Invalid with **`-k`**.

-e displays the encryption types of the session key and the ticket for each credential in the credential cache (by default), or each key in the keytab file (if **-k** is specified).

-f shows the flags present in the credentials, using the following abbreviations:

A	preAuthenticated
F	Forwardable
f	forwarded
P	Proxiable
p	proxy
D	postDateable
d	postdated
R	Renewable
I	Initial
i	invalid

Requires **-c**. Invalid with **-k**.

-k lists keys held in a keytab file (as opposed to tickets in a credentials cache). Keytab files are generally used for service principals. Invalid with **-c**.

-K displays the value of the encryption key in each keytab entry in the keytab file. Invalid with **-c**.

<keytab_name> specifies the keytab file. If **<keytab_name>** is not specified, **klist** will display the keys in the default keytab file (unless instructed to operate on a credentials cache). Invalid with **-c**.

-R does not reverse-resolve[1]. Requires **-a** (and thus **-c**). Invalid with **-k**.

-s causes **klist** to run silently (produce no output), while still setting the exit status according to whether it finds the credentials cache. The exit status is "0" if **klist** finds a credentials cache, and "1" if it does not. Requires **-c**. Invalid with **-k**.

-t displays the time entry timestamps for each keytab entry in the keytab file. Invalid with **-c**.

1. To reverse-resolve involves getting a message (i.e. kerberos ticket or email) with an originating IP address. The recieving machine then would check the IP address with the nameserver (DNS). The -R option skips this test/check.

-4	lists only Kerberos v4 tickets/keys (default lists both 4 and 5)
-5	lists only Kerberos v5 tickets/keys (default lists both 4 and 5)

12.2.3 Examples

Most frequently this command is issued with the **-f** option to indicate the flags set on each ticket:

```
% klist -f
   Ticket cache: /tmp/krb5cc_ttyp0
   Default principal: aheavey@FNAL.GOV

   Valid starting     Expires            Service principal
   02/11/00       12:45:33              02/12/00       01:45:33
   krbtgt/FNAL.GOV@FNAL.GOV
           Flags: FIA
   02/11/00 12:45:33  02/12/00 01:45:33  afs/fnal.gov@FNAL.GOV
           Flags: FA
```

To list the keys in a keytab file (for example a keytab file created for use with a **cron** job, see section 10.3.1 *Specific-User Processes (cron Jobs)*), use the **-k** and **-t <filename>** options:

```
% klist -k -t /usr/tmp/user1.keytab
   Keytab name: FILE:/usr/tmp/user1.keytab
   KVNO Timestamp         Principal
   ----                                           -----------------
   -------------------------------------------------------------
      9 02/15/00 10:34:28 user1/cron@FNAL.GOV
```

12.3 kpasswd

The **kpasswd** command is used to change a Kerberos principal's password. You can change a principal's password from any account on a machine in the realm. **kpasswd** prompts for the current Kerberos password, and if supplied correctly, the user is then prompted twice for the new password, and the password is changed. **kpasswd** works even if the old password has expired.

In the FNAL.GOV realm, a policy is in effect that specifies the length and minimum number of character classes required in the new password. The password must be at least ten characters long and contain at least two character classes. For *root*, the password must contain at least 13 characters of at least three classes. The character classes are: lower case, upper case, numbers, punctuation, and all other characters.

12.3.1 Syntax

```
% kpasswd [<principal>]
```

12.3.2 Argument Description

<principal> Change the password for the Kerberos principal **<principal>**. If not given, the principal is derived from the identity of the user invoking the **kpasswd** command.

12.4 kdestroy

The **kdestroy** utility destroys the user's active Kerberos credentials (tickets) by writing zeros to the specified credentials cache that contains them, and then deleting the cache. If the credentials cache is not specified, the default credentials cache specified by $KRB5CCNAME is destroyed.

12.4.1 Syntax

```
% kdestroy [-q] [-c cache_name] [-4] [-5]
```

12.4.2 Option Descriptions

-q Runs quietly. Normally **kdestroy** beeps if it fails to destroy the user's tickets. The **-q** flag suppresses this behavior.

-c <cache_name>

Uses **<cache_name>** as the credentials (ticket) cache name and location; if this option is not used, the default cache name and location are used. If the $KRB5CCNAME environment variable is set, its value is used to name the default cache. At Fermilab, this variable is typically set to **FILE:/tmp/krb5cc_<some_string>**.

-4 destroys only Kerberos v4 tickets/keys (default destroys both 4 and 5)

-5 destroys only Kerberos v5 tickets/keys (default destroys both 4 and 5)

12.5 Kerberized su (ksu)

Be aware that you need to have a host principal in order to use ksu. See section 14.1.6 *Do you Need to Allow Incoming Kerberos Connections?* about host principals.

12.5.1 Syntax

The following discussion is adapted from the **ksu** man pages. See them for more information, in particular for option descriptions. The command syntax is:

```
% ksu [<target_user>] [-n <target_principal_name>] \
 [-c <source_cache_name>] [-C <target_cache_name>] [-k] [-D]\
 [-r <time>] [-pf] [-l <lifetime>] [-zZ] [-q]\
 [-e <command> [<args ...>]] [-a [<args ...>]]
```

12.5.2 Description

The Kerberos V5 **ksu** program is a Kerberized version of the **su** program that has two missions: one is to securely change the real and effective user ID to that of the target user, the other is to create a new security context.

To fulfill the first mission, **ksu** operates in two phases: authentication and authorization. Resolving the target principal name is the first step in authentication. If the source user is *root* or the target user is the source user, no authentication or authorization takes place. In all other cases, **ksu** looks for an appropriate Kerberos ticket in the source cache. If no ticket is in the cache, then depending on how **ksu** was compiled, the user may be prompted for a Kerberos password.

Make sure you are logged in using an encrypted connection before typing your password!

Upon successful authentication, **ksu** checks whether the target principal is authorized to access the target account. In the target user's home directory, authorization is based on whether appropriate entries exist in either `.k5login` or `.k5users`, or by name-mapping rules if neither file exists.

ksu can be used to create a new security context for the target program. The target program inherits a set of credentials from the source user. By default, this set includes all of the credentials in the source cache plus any additional credentials obtained during authentication. The source user is able to limit the credentials in this set.

12.5.3 Option Descriptions

More complete option descriptions are available at the **ksu** man page.

-n target_principal_name; if **ksu** is invoked without **-n**, a default principal name is assigned

-c source_cache_name; if **-c** option is not used then the name is obtained from KRB5CCNAME environment variable.

-C target_cache_name

-k Do not delete the target cache upon termination of the target shell or a command (**-e <command>**).

-D turn on debug mode.

Ticket granting ticket options:

-l <lifetime> option specifies the lifetime to be requested for the ticket; if this option is not specified, the default ticket lifetime (configured by each site) is used instead.

-r <time> option specifies that the RENEWABLE option should be requested for the ticket, and specifies the desired total lifetime of the ticket.

-p specifies that the PROXIABLE option should be requested for the ticket.

-f option specifies that the FORWARDABLE option should be requested for the ticket.

-z restrict the copy of tickets from the source cache to the target cache to only the tickets where client = the target principal name. Use the **-n** option if you want the tickets for other then the default principal. Note that the (lower case) **-z** option is mutually exclusive with **-C** and (upper case) **-Z** options.

-Z Don't copy any tickets from the source cache to the target cache. Just create a fresh target cache, where the default principal name of the cache is initialized to the target principal name. Note that (upper case) **-Z** option is mutually exclusive with **-C** and (lower case) **-z** options.

-q suppress the printing of status messages.

-e command [args ...] **ksu** proceeds exactly the same as if it was invoked without the **-e** option, except instead of executing the target shell, **ksu** executes the specified command.

-a args specify arguments to be passed to the target shell. All options intended for **ksu** must precede **-a**.

12.6 kvno

The **kvno** command acquires a service ticket for the specified Kerberos principals and prints out the key version numbers of each. It uses the variables KRB5CCNAM (location of the credential cache) and KRBTKFILE (location of the v4 ticket file).

12.6.1 Syntax

```
% kvno [-q] [-h] [-4 | [-c <ccache>] [-e <etype>]] \
  <service1> <service2> ...
```

12.6.2 Option Descriptions

-c <ccache> specifies the name of a credentials cache to use (if not the default). Invalid with **-4**.

-e <etype> specifies the enctype[1] which will be requested for the session key of all the services named on the command line. This is useful in certain backward compatibility situations. Invalid with **-4**.

-q suppresses printing

-h prints a usage (help) statement and exits

-4 specifies that Kerberos version 4 tickets should be acquired and described. This option is only available if Kerberos 4 support was enabled at compilation time.

1. From the Mozilla development center web page: DOM:form.enctype gets/sets the content type of the FORM element.